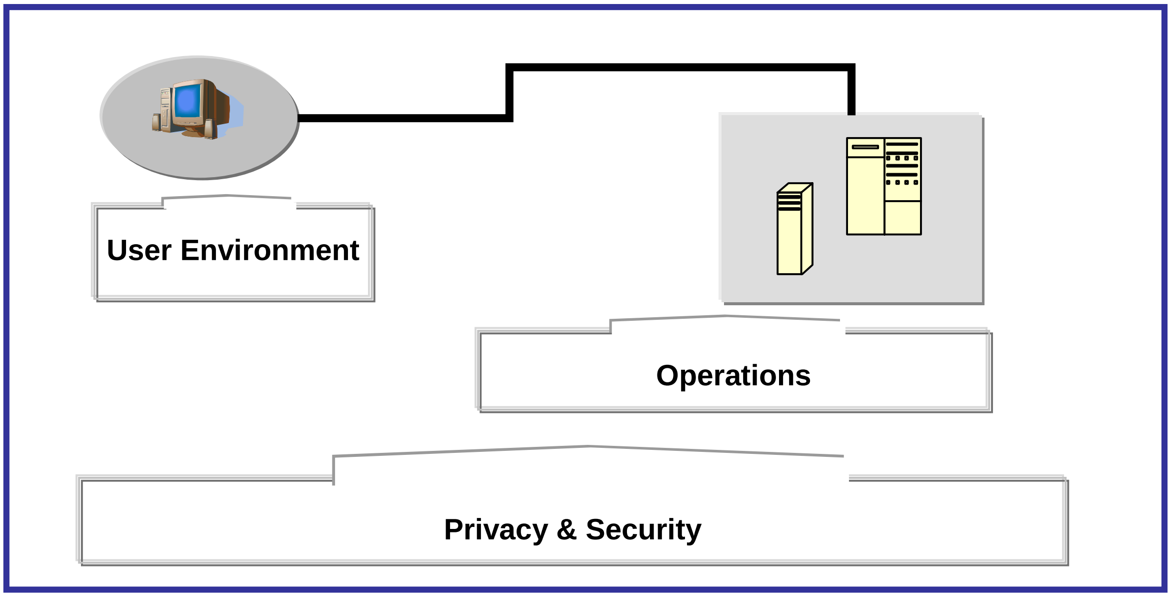
Technology and Security Resource Guide

Work Away Advisory Committee
Technology Subcommittee
January 2005

Work Away Resource Guide

Preface



Work Away Program

Working from home or other alternate locations can benefit our environment, the state, and employees. However, with the extension of the work environment to alternate work locations, technical requirements and security safeguards are required for a productive and secure work environment.

Resource Guide

This guide provides a collection of information compiled by and for agencies to address common technical and security related elements for work away programs. Its purpose is to equip agency personnel to make informed decisions regarding implementation and management of their programs. It is not exhaustive nor prescriptive for agency implementations; rather, agencies must evaluate their own environment, the risks involved, and their available resources for any decision to provide and support teleworking.

The guide was compiled and developed by the Work Away Technical Subcommittee and is divided into 3 sections: Privacy & Security, User Environment, and Operations. In each section items to consider for remote access are provided, along with documents/templates/resources for use by the agency.

Conclusion

It is our hope that the document provides agencies with assistance for the technical and security requirements necessary in deploying successful work away programs that benefit the employee and protect the resources of the state.

Work Away Resource Guide

Acknowledgements

The Technology Committee of the Work Away Program consists of members from supporting organizations who have provided their time and resources for the development and publishing of the resource guide. Team members include:

- Renee Herr, GTA – Chairperson
- Deborah Belcher, GMS
- Lynn Bolton, DOAA
- Larry Bray, GTA
- Dorothy Gordon, GMS
- Bob Grafals, GTA
- Bill Gray, DTAE
- Jeremy Hopwood, The Clean Air Campaign
- Mark Pruitt, DMVS
- Naomi Richardson, GTA
- David Rierson, GDA
- Lisa Sharpton, GDEcD
- Sherri Southern, GTA
- Shannon Thompson, GTA
- Chris Tomlinson, GTA
- Cherri Tucker, DCH
- Beverly Walker, GTA
- Robert Woodruff, GTA
- Al Yelverton, GTA

The Technology Committee also would like to gratefully acknowledge the contribution of the following agencies for the use of their documents and other assistance in the development of the resource guide:

- Department of Natural Resources
- Department of Audits
- Department of Community Affairs
- Georgia Bureau of Investigation
- Georgia Public Broadcasting
- Georgia Department of Corrections

Work Away Resource Guide

Table of Contents

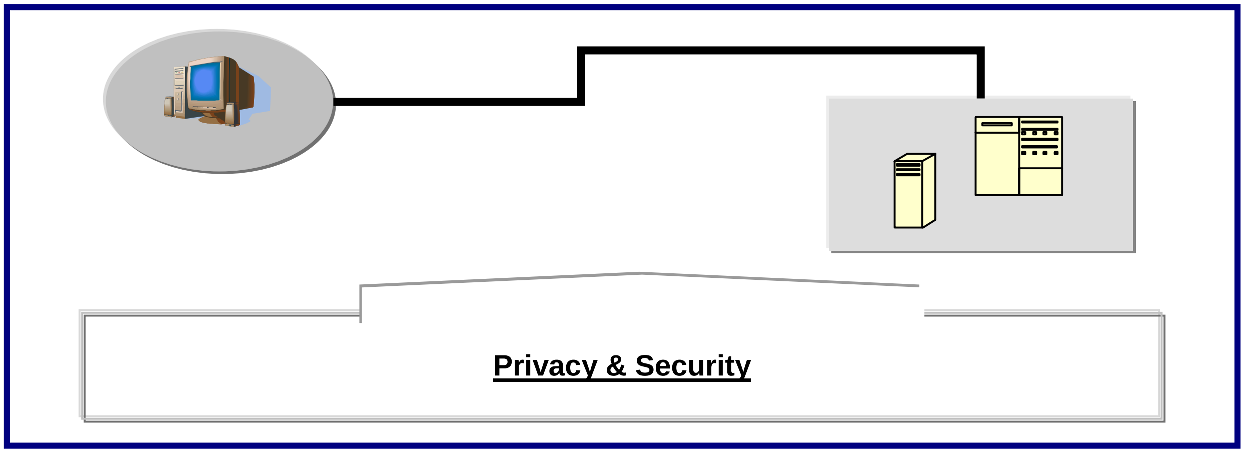
Section 1 – Privacy & Security

Section 2 – User Environment

Section 3 – Operations

Appendix

Section 1: Privacy & Security



The privacy and security of information used by teleworkers is paramount for remote access and offices. Safeguards and controls are a vital part of compliance with state and federal regulations that govern the storage, access, and transmission of confidential or sensitive information. This section of the resource guide provides links to documents and practices that are valuable tools for protecting the confidentiality and security of state data and assets.

1.1 Privacy & Security

Policies and other documents are necessary in the Work Away program to specify the expectations and requirements of the agency and the responsibilities of the employee. Policies, acknowledgements, and checklists for teleworking are contained in the GMS Work Away Telemanager and Teleworker Training documents. In addition, security policies should be implemented and maintained through the security organization in each agency as specified in the Enterprise Policies.

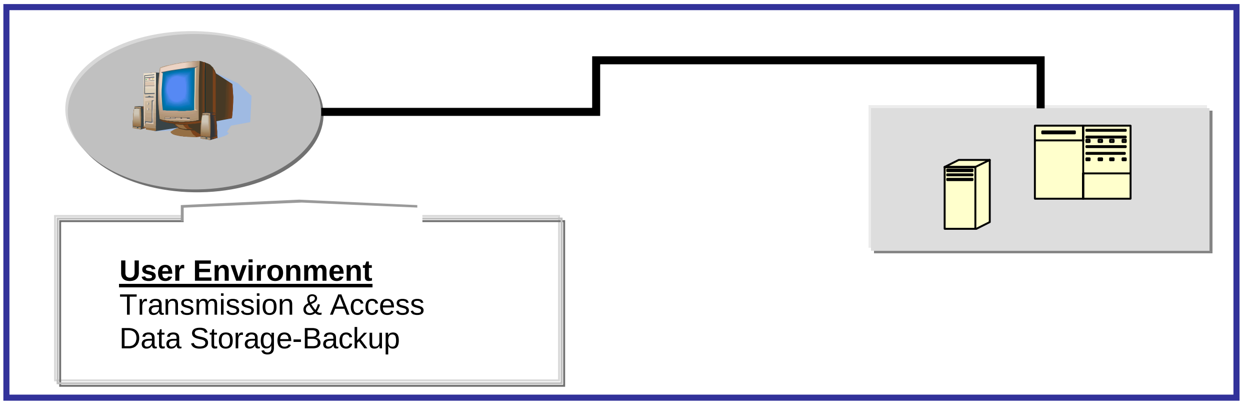
Privacy and security requirements are incorporated and specified in regulations issued by the Federal government regarding such areas as health, education, taxes, etc. The regulations specify that certain types of data must be protected from unauthorized access, improper alteration, or disruption in availability.

1.2 Resources

Teleworker environments are required to meet security and privacy requirements incorporated in policies and regulations. The resources list below contains documents and websites for policies, standards, and whitepapers on security for remote access and telework environments.

Security Policies	Policies govern and specify the safeguards and controls to ensure safe and productive remote access; these controls cover a wide array of topics for ensuring the confidentiality, integrity, and availability of the data and state resources. Enterprise Policies are found on the GTA website, *Enterprise Information Security Policy* (http://gta.georgia.gov/00/channel_modifieddate/0,2096,1070969_7295376,00.html).
GMS Teleworker Resources	Helpful documents for the teleworker and manger of teleworkers, including statewide policy, training materials, teleworker agreements, etc. (http://www.gms.state.ga.us/employee/telework.asp)
Privacy Whitepaper	The Secretary of State published a paper in 2004 from a symposium held with members of the private and public sectors; the paper describes state recommendations regarding privacy and the Open Records Act; the paper is available at the Secretary of State website, *Protecting Personal Information* (www.sos.state.ga.us/archives/rms/paer.htm)
Regulations	Federal regulations specify the safeguards necessary for access, transmission, and storage of certain types of information (e.g., health, financial, education, and law enforcement). These requirements can be found under HIPAA, GLBA, FERPA, and CJIS at federal and/or private websites.
GTA Enterprise Information Security Procedures	Provides a uniform set of information security policies, standards and general guidelines for State of Georgia agencies. **All Agencies, as that term is defined in the Official Code of Georgia Annotated § 50-25-1(b)(1), unless specifically exempted, are required to abide by the policies hereby established. All users (employees, contractors, vendors, and other parties) are expected to understand and abide by them.** http://gta.georgia.gov/vgn/images/portal/cit_1210/62/58/1218035EnterpriseInforSecurityPoliciesGEITLF.pdf

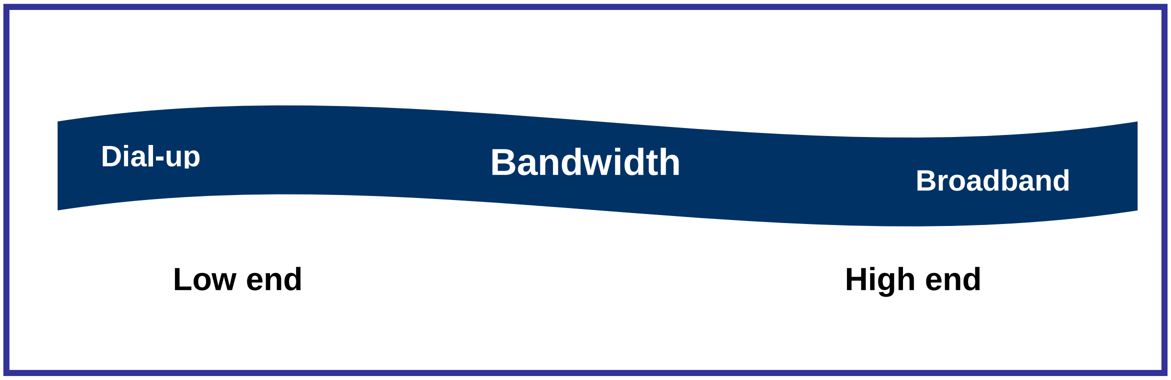
Federal Standards-Best Practices	The National Institute of Science and Technology (NIST) has published numerous documents that provide useful information on security practices and procedures. (http://csrc.nist.gov/publications/nistpubs/index.html; http://csrc.nist.gov/publications/drafts.html#sp80053)



Access for the teleworker to the State network entails the transmission of the data and the method of connection used. The type of transmission is a variable based on choice and availability for the teleworker's local service provider, with the access method most often determined by the agency for the functions to be performed. The security of the access varies from user authenticated sessions to secure-encrypted connections, with third party alternative packages also. Teleworkers may use one or more connection methods from their remote sites. This section of the resource guide breaks down the options based on the transmission options, then by connection solutions.

2.1 Transmission

The type of transmission option used can differ based on the availability of the service in the remote area and the needs of the teleworker. The broadband option includes both DSL, cable modem and wireless provides higher access speeds, but also comes with the need for additional controls to prevent unauthorized access to the equipment at the teleworker location.



Dial-up

Uses basic phone lines and transmission facilities to connect to the state network or websites; these connections are slower and are somewhat less frequently the target of unauthorized access via the internet, but still need to have protective measures to insure that malicious code (e.g., viruses, worms, etc.) are not introduced into the state environment.

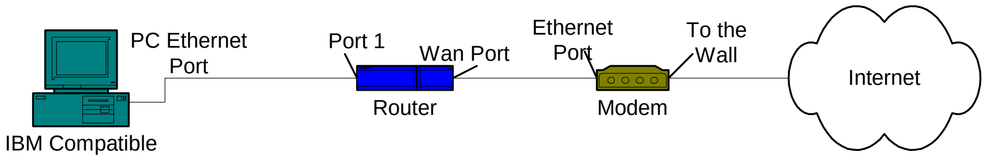
Dial-up	
Safeguards	**Description**
Antivirus Software	Software that detects the presence of malicious software and prevent infection to the machine; updates are critical to keep the virus signatures current.
Personal Firewall	The firewall provides for rules to be established that will prohibit certain traffic; this is useful to block attacks or detect if they are occurring.

Broadband, Wireline

Consists of DSL and cable modems. These devices offer increased rates of transmission, but also have features, such as always-on-access, that require increased levels of security to protect state assets and access.

Broadband	
Safeguards	**Description**
DSL/Cable Router	The router provides an additional level of security for access. (Also may provide functionality for authentication and encryption with VPN options.)
Personal Firewall	The firewall provides for rules to be established that will prohibit certain traffic.
Antivirus Software	Software that detects the presence of malicious software and prevent infection to the machine; updates are critical to keep the virus signatures current.
Ethernet adapter	Adapter used for router connection for the router-modem connection.

Below is a diagram of the configuration for the router and Ethernet adapter described for the broadband connection.

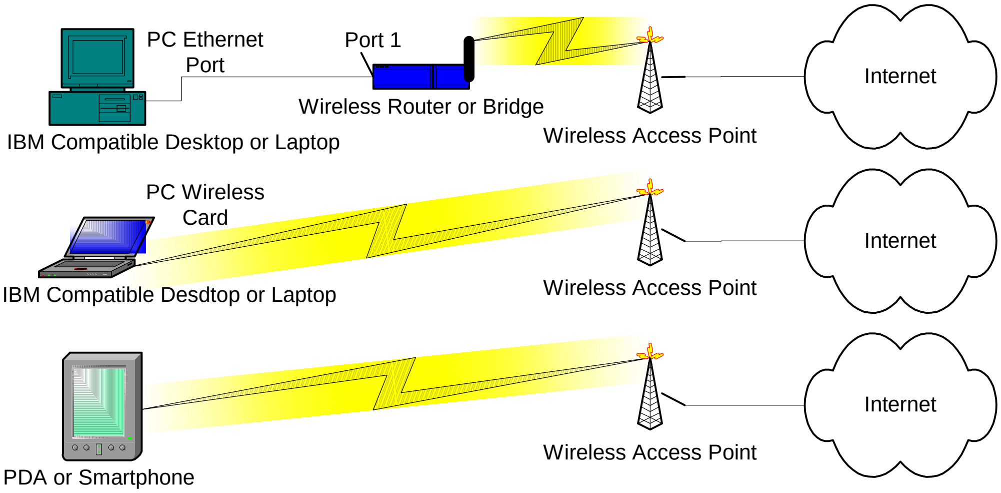


Broadband, Wireless, 802.xx

Consists of wireless router or wireless PC card. These devices offer increased rates of transmission, but due to their “over the air” broadcast nature and features, such as always-on-access, require increased levels of security to protect state assets and access.

Broadband, Wireless, 802.xx	
Safeguards	**Description**
Wireless Router or Bridge	The wireless router or Bridge provides an additional level of security for access when authentication, authorization & accounting are deployed using strong security protocols (EAP, LEAP, PEAP, TTLS, etc.), encryption (WEP, WPA, WPA2 & AES), lock-down measures and RF monitoring & rogue access point & client detection. (Also may provide functionality for authentication and encryption with VPN options.)
Wireless PC Card	The wireless PC card provides an additional level of security for access when authentication, authorization & accounting are deployed using strong security protocols (EAP, LEAP, PEAP, TTLS, etc.), encryption (WEP, WPA, WPA2 & AES), lock-down measures and RF monitoring & rogue access point & client detection. (Additional software may be required to provide functionality for authentication and encryption with VPN options.)
Personal Firewall	The firewall provides for rules to be established that will prohibit certain traffic.
Antivirus Software	Software that detects the presence of malicious software and prevent infection to the machine; updates are critical to keep the virus signatures current.
Ethernet adapter	Adapter used for router connection for the PC-wireless router connection.
PDA and Smartphone	The PDA and Smartphone provides an additional level of security for access when authentication, authorization & accounting are deployed, however most don’t support strong security protocols (EAP, LEAP, PEAP, TTLS, etc.) and encryption (WEP, WPA, WPA2 & AES), Additional lock-down measures and RF monitoring & rogue access point & client detection should be deployed. (Additional software may be required to provide functionality for authentication and encryption with VPN options if available.)

Below are diagrams of the configuration for the wireless router or bridge, wireless PC card and PDA or Smartphone described for the wireless connection.


PC Ethernet Port
Port 1
Wireless Router or Bridge
IBM Compatible Desktop or Laptop
Wireless Access Point
Internet
PC Wireless Card
IBM Compatible Desdtop or Laptop
Wireless Access Point
Internet
PDA or Smartphone
Wireless Access Point
Internet

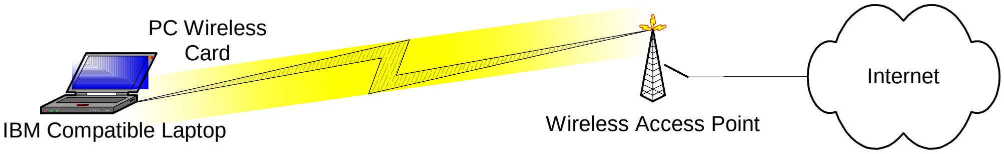
Broadband, Wireless 3G

CDMA2000-1x/Evolution-Data Only (EV-DO) (Verizon, Sprint)

Consists of a wireless laptop card. This device offers increased rates of transmission, but due to their “over the air” broadcast nature and features, such as always-on-access, require increased levels of security to protect State assets and access.

Broadband, Wireless 3G, EV-DO	
Safeguards	**Description**
Wireless Laptop Card	The wireless laptop card provides an additional level of security for access when authentication, authorization & accounting are deployed. EV-DO uses CDMA technology, which provides authentication and data protection and works with most VPN solutions. Uses a wireless PC 5220 card available for laptop only. (Additional software may be required to provide functionality for authentication and encryption with VPN options if available.)
Personal Firewall	The firewall provides for rules to be established that will prohibit certain traffic.
Antivirus Software	Software that detects the presence of malicious software and prevent infection to the machine; updates are critical to keep the virus signatures current.

Below are diagrams of the configuration for the wireless laptop card described for the wireless connection.

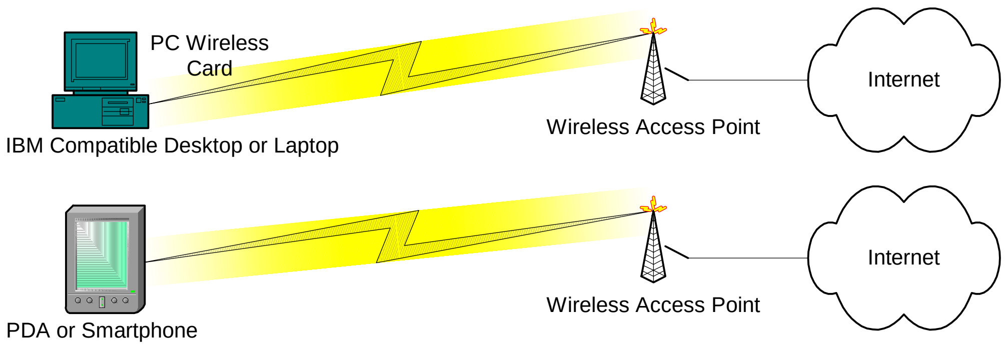


iDEN / WiDEN (Southern LINC / Nextel)

Consists of a wireless PC card or data capable handset. These devices offer increased rates of transmission, but due to their “over the air” broadcast nature and features, such as always-on-access, require increased levels of security to protect state assets and access.

Broadband, Wireless 3G, iDEN / WiDEN	
Safeguards	**Description**
Wireless PC Card	The wireless PC card provides an additional level of security for access when authentication, authorization & accounting are deployed. iDen/WiDEN uses GPRS technology, which provides authentication and data protection and works with most VPN solutions. Wireless cards are available for desktop & laptop PCs. (Additional software may be required to provide functionality for authentication and encryption with VPN options if available.)
Personal Firewall	The firewall provides for rules to be established that will prohibit certain traffic.
Antivirus Software	Software that detects the presence of malicious software and prevent infection to the machine; updates are critical to keep the virus signatures current.
PDA and Smartphone	The PDA and Smartphone provide an additional level of security for access when authentication, authorization & accounting are deployed. iDEN/WiDEN uses GPRS technology, which provides authentication and data protection and works with most VPN solutions. (Additional software may be required to provide functionality for authentication and encryption with VPN options if available.)

Below are diagrams of the configuration for the wireless PC card, PDA or Smartphone described for the wireless connection.



2.2 Access Scenarios

The various options for remote access have been combined into common scenarios for the user environment. The scenarios provide the description and pros/cons for each. The access solutions are dictated by the nature of the data/applications to be accessed, and the support-cost considerations. The products listed in each section are ones commonly used or in various stages of evaluation/procurement.

Dial-up
Bandwidth
Broadband

Server Based	**VPN SSL**
Remotely Managed	**VPN IPSec**
Dial-up Services	**802.xx: EAP, LEAP, PEAP, etc. w/ WEP, WPA, WPA2, AES**
	CDMA-2000/EV-DO
	iDEN/WiDEN

2.2.1 Low End Bandwidth Scenarios

Using dialup, the teleworker has a more limited set of scenarios to access from the remote location. These options can also be used with the higher end bandwidth transmissions. The more common solutions available are listed below with the related pros and cons.

Server Based

This scenario is a server based computing-to-heterogeneous computing environment and provides access to standard windows 32 bit programs regardless of client hardware, operating environment, network connection, or protocol. The remote worker will connect, and login to the network just as they do at the office – however, unlike some other functions, all user sessions reside on the server.

Server Based		
Pros		
	Ease of use	Gives workers secure, easy and instant access to enterprise applications, information, processes and people, no matter where they are located, from anywhere, at anytime, using any device, over any connection.
		Web-enables applications
	Support	Central management Enables IT staffs to manage heterogeneity by enabling the centralized management of applications, simplifying their deployment, monitoring and measurement.

		Maintenance and support reductions Support staff simply supports the same desktop that they do currently. No requirement to bring computer in, or meet for repairs, or deploy to remote location.
		Potential to reduce costs Reduced licensing costs; easily move single-seat licenses, operating system/duplicate software licenses
		Software deployment No need to push to remote location, use the LAN – no worries of bandwidth issues.
	Security	Ability to lock down desktop
		Reduce virus exposure Computers are still on corporate LAN – where controlled/monitored.
		More Control Ensures that only the right people have access to the right resources to protect the security of enterprise information assets.
Cons		
	Costs	Very expensive to build the Citrix Server (hardware), additional cost including cost of Citrix software. Cost and support are two largest reasons why this solution is not chosen.
	Support	Need to have someone very familiar with the product, or certified to install. Need to have expertise to setup to work with all environment variables.
		Learning curve for support people Adds a level of complexity to the infrastructure. Server farm-n-tier environment
		Application support Not all applications are Thin Client-aware; some must stay local.
		Legacy applications Not all applications will work with Citrix.
	End-user	Complexity Have to train users or control where things are stored so they can access all data at all locations.
		Graphics Very low level – not acceptable for some positions such as designers.
		Drives Local drives such as CDROM not present.
Products		**Citrix**

Remotely Managed

Remotely managed services allow users to access the desktop computer from any other Internet-connected computer with almost any operating system through a secure, private connection. Requires software to be installed on the Host computer; access from remote computer is achieved by signing on through the remotely managed website.

Remotely Managed		
Pros		
	Scale	Can build a program with as small as 1 user.
	Cost	If have a small program – cost can be less than other solutions.
	Personal computer	Because the solution is more of a "remote control" scenario.
	Low bandwidth	Dial-up analog is sufficient.
Cons		
	Cost	Cost per user, may be a problem for scalability for large user populations.
	Complex sign-on	Requires 4-5 steps to sign on.
	Security	Security has been improved over the past few years. Needs assessment to determine if it matches security requirements.
Products		**GoToMyPC**

Dial-up (RAS) Solutions

Standard RAS or “Remote Access Server” infrastructure is a “direct connection” solution. The remote computer would dial a private line telephone number to the server and once authenticated, establish a point-to-point connection.

RAS		
Pros		
	Security	Excellent security measures because of “on-demand” access. Multiple security protocols and mechanisms perfected over the years.
	Scale	Good solution for very small teams where costs can be controlled.
	Reliable	Not a shared resource, therefore solid communication paths.
Cons		
	Scale	Leased lines and point-to-point solutions require multiple resources from providers – causing the costs to sky-rocket. Single largest reason why this solution is not chosen anymore.
	Single Point of Failure	If the line goes down, service interrupted, unlike internet-based solutions.
	Support	Costly to support because of the interdependence of carriers, and the one-to-one style architecture.
Products		

2.2.2 High End Bandwidth Scenarios

Broadband provides higher speed connections and encryption, and should follow the recommended configuration described previously for secure connections. The higher speeds enable encryption options for more security communications.

VPN Solutions

VPN technology is based on the idea of tunneling. Network tunneling involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side.

VPN		
Pros		
	Accessibility	Compared to leased lines, Internet-based VPNs offer greater global reach, given that Internet access points are accessible in many places where dedicated lines are not available.
	Cost	Another way VPNs reduce costs is by lessening the need for long-distance telephone charges for remote access. Also elevates the need for expensive long-distance /leased lines.
	Support	With VPNs, the service provider rather than the organization must support dial-up access.
	Security	Multiple platforms to meet security needs PPTP, L2TP, IPSEC, SSL
		Flexible encryption algorithms DES, 3DES, PKI
	Scalable	Most VPN solutions can scale to meet the needs of any size organization easily.

Cons		
	Support	Higher level of skills required VPNs require an in-depth understanding of public network security issues and taking proper precautions in VPN deployment.
		Interdependence The availability and performance of an organization's wide-area VPN (over the Internet in particular) may depend on factors largely outside of their control.
	Single-Platform solution	VPN technologies from different vendors may not work well together due to immature standards
	Bandwidth	Typically, requires more bandwidth than other solutions. (Broadband)
	Cost	More costly to implement than other solutions – TCO can be higher depending on the type VPN solution chosen and the policy concerning personal computers.
	Company equipment	If software client deployed on personal computer, then network is compromised – should only be deployed with company controlled asset.
	Legacy applications/protocols	VPNs need to accommodate protocols other than IP and existing ("legacy") internal network technology.
Options		
VPN IPSec (pilot)		
	Workstation to Data Center-client-to-site (C2S); remote client	Requires client or devices at remote site; increased admin for client software; possible Network Address Translation (NAT) problems.
	LAN to Data Center-site-to-site (S2S); remote device	
VPN SSL		
	LAN to Data Center-site-to-site (S2S); remote device.	Used for web-based communications; all traffic encrypted
Products		**NetScreen**

Comparison of IPSec vs. SSL VPNs		
IPSec		
	Advantages	• IPSec provides full use of network resources including legacy applications • Unique client on user device enhances authentication • Application agnostic including VoIP
	Limitations	• Requires client software installation/management • Needs firewall reconfiguration/compatibility • Might provide too much access
	Ideal Applications	• Site-to-Site VPNs • Some teleworker VPNs • Voice AND Data traffic
SSL	Advantages	• 'Clientless' extranet solution allows freedom of remote access device • Provides tight access control because session is specific to an application/server • Network agnostic
	Limitations	• Limited applications – Typically limited to 'web' applications – primarily HTTP • SSL Handshake slows performance • One session per application, i.e. multiple sessions if need for many apps • Not suitable for voice traffic
	Ideal Applications	• Enterprise Application Portals • eBusiness Applications (B2C/B2B)

2.3 Data Storage-Backup

Data downloaded by the teleworker for use at the remote site, printed or stored on media must be secured against unauthorized access or disruption due to destruction or loss.

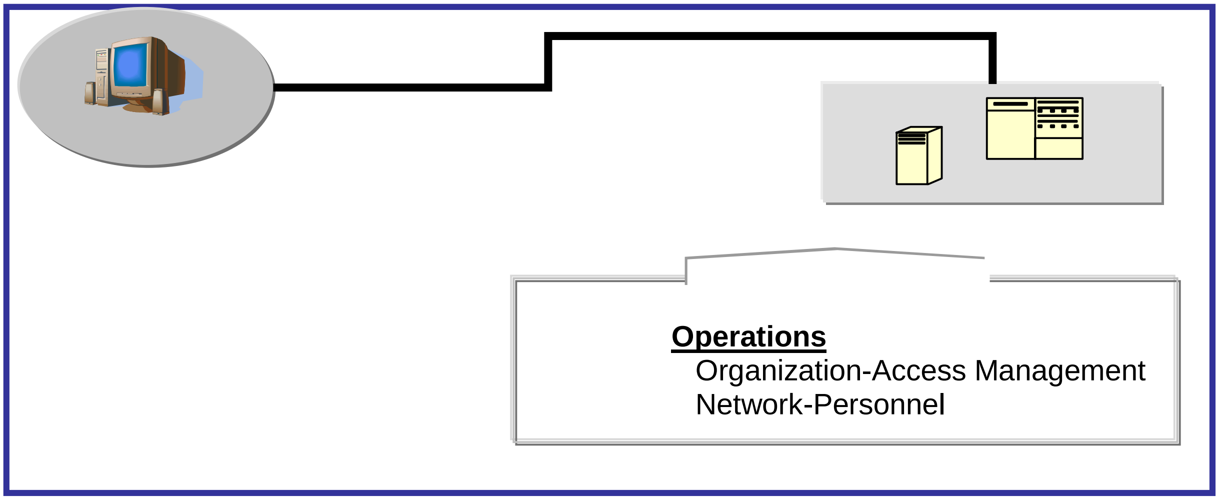
Data Storage-Backup		
Laptop security	Access controls - physical controls	Encryptions or security devices to protect against theft or loss, and access.
Printouts & portable media	Secure storage and destruction	Physical security and environmental controls based on nature of items and confidentiality; shredder for materials no longer in use
Backups	Backups of data	Copies at specified intervals; recovery copies secured and stored at alternate location

2.4 Records Retention

Records and documents used by the teleworker at the remote site are subject to the same requirements as documents in the primary work location. The documents are covered by the Open Records Act and may be required to be provided as requested. These requirements also apply to state documents stored on an employee's personal equipment at the remote site.

Records Retention		
Retention	Retention requirements	Retention of records created and/or stored at remote sight to match specifications of office environment.
Open Records	Requests	Records are accorded the same requirements for retrieval as those on state equipment and at office location.

Section 3: Operations



3.1 Operation Controls

Operations provide the controls and processes for remote access and the organization structure for its management. The controls include areas for organization, data categorization and access, and network operations, i.e., the work behind the scenes for effective telework practices.

Organization: Administration and management oversight for controls.	
Admin role	Assigned responsibility for administration and participation
Security	Assigned responsibility for security-policies-procedures-safeguards
Inspection	Process for inspection and validation of safeguards, onsite or remote

Administration and management of the telework program must be assigned within the Agency to ensure ongoing support and diligence for secure computing. The responsibilities should be documented and updated as the functions evolve based on the nature of the access and functions performed in the program.

Access Management: Categorization and approvals for access.	
Data categorization	Categorization of data based on restrictions specified by regulation, law or policy, with data owners
Privilege access	Differentiation of access levels based on job function with access approval

Access management for the data and functions involves both the categorization of the data to be accessed and the process for add-change-delete of access for the teleworker community. The data categorization is necessary to differentiate the types of data accessible electronically and ensure proper protection is afforded it to prevent unauthorized access.

Network: Monitoring activity and infrastructure to support.	
Audit logs	Logging of activity with review, investigation, and response
Design	Placement of access devices to ensure safeguards for availability, integrity, and access

Network operations involve the review and follow up of audit logs that reflect activity on the network that would indication a security incident. Also, an operation includes the placement of access points and the protective devices on the network for alerts and alarms of security incidents.

Personnel: Preparation and contact for reporting incidents.	
Training and awareness	Orientation to the policy, procedures and expectations
Incident reporting	Process for reporting security incidents involving attempted or actual unauthorized access or loss of availability.

Personnel measures to support teleworking involve the awareness and training of teleworkers as part of the overall security training program. In addition, the teleworkers must be informed of ways to recognize security events and the proper channels for reporting such suspected incidents.

Work Away Resource Guide

Appendix

A. Technology and Security Checklist

Category	Topic	Description		✓
Privacy & Security	**Policy**	Security policies		
	Privacy	Privacy and handling requirements		
	Regulations	Federal and state regulations		
User Environment	**Transmission**	Dial-up	Antivirus	
			Firewall	
		Broadband, Copper	DSL/Cable Router	
			Personal Firewall	
			Antivirus Software	
			Ethernet adapter	
		Broadband, Wireless, 802.xx	Wireless Router	
			Wireless PC Card	
			Personal Firewall	
			Antivirus Software	
			Ethernet adapter	
			PDA or Smartphone	
		Broadband, Wireless, EV-DO	Wireless Laptop Card	
			Personal Firewall	
			Antivirus Software	
		Broadband, Wireless, iDEN/WiDEN	Wireless PC Card	
			Personal Firewall	
			Antivirus Software	
			PDA or Smartphone	
	Access	Server Based		
		Remotely Managed		
		Remote Access Server (Dial-up)		
		VPN		
	Data Storage-Backup	Laptop security		
		Printouts & portable media		
		Backups		

	Records Retention	Retention and access for Open Records	
Operations	**Organization**	Administration	
		Security management	
		Inspection	
	Access Mgt.	Data classification	
		Privilege access	
	Network	Audit logs (network and remote)	
		Network design-remote access points	
	Personnel	Training and awareness	
		Incident reporting	

B. General References

I. ISO 17799

II. NIST Publications
http://csrc.nist.gov/publications/nistpubs/index.html

NIST 800-46 Security for Telecommuting and Broadband Communications

NIST 800-48 Wireless Network Security

NIST 800-49 Federal S/MIME V3 Client Profile

FIPS 140-2 Federal Information Processing Standard (Maintained by NIST)

III. ANSI/IEEE Standard 802.2, 1998 Edition, and ISO/IEC 8802-2:1998.

IEEE 802 General Information
http://www.ieee.org/portal/site/mainsite/menuitem.818c0c39e85ef176fb2275875bac26c8/index.jsp?&pName=corp_level1&path=about/802std&file=index.xml&xsl=generic.xsl

IEEE 802.11 - is a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

IEEE 802.11 - applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

IEEE 802.11a - an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band; but most commonly, communications takes place at 6 Mbps, 12 Mbps, or 24 Mbps. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS. The specification applies to wireless ATM systems and is used in access hubs.

IEEE 802.11b - often called Wi-Fi - is backward compatible with 802.11. The modulation used in 802.11 has historically been phase-shift keying (PSK). The modulation method selected for 802.11b is known as complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference.

IEEE 802.11g - applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.

IEEE 802.11x (802.11e, f, h, i) Wireless Local Area Network (WLAN) Standards

IEEE 802.11e - adds quality-of-service (QoS) features and multimedia support to the existing IEEE 802.11b and IEEE 802.11a wireless standards, while maintaining full backward compatibility with these standards.

IEEE 802.11f – adds Access Point Interoperability (future)

IEEE 802.11h – adds Interference (future)

IEEE 802.11i - adds the Advanced Encryption Standard (AES) security protocol to the 802.11 standard for wireless LANs. Two encryption modes: TKIP + MIC and AES.

IEEE 802.15 - Wireless Personal Area Networks

IEEE 802.15a Wireless Personal Area Network - Bluetooth

IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX)

IEEE 802.16e (Emerging Mobile Version)

IEEE 802.16n (Future)

IEEE 802.20 Mobile Broadband Wireless Access (MBWA)

MIMO Multiple Input-Multiple Output (Under Development)

IV. CDMA Development Group (CDG) CDMA2000 1xEV-DV

TIA/EIA/IS-2002.3-C, Medium Access Control (MAC) Standard for cdma2000
Spread Spectrum Systems, May 2002.

TIA/EIA/IS-2000.5-C, Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems, May 2002.

TIA/EIA-97-D, Recommended Minimum Performance Standards for Base Stations Supporting Dual-Mode Spread Spectrum Mobile Stations, April 2001.

TIA/EIA-98-D, Recommended Minimum Performance Standards for Dual-Mode Spread Spectrum Mobile Stations, April 2001.

S.S0055 v1.0, Enhanced Cryptographic Algorithms, January 2002

TSB58-E, Administration of Parameter Value Assignments for cdma2000 Spread Spectrum Standards, Release C, January 2002.

V. ANSI C.95.1-1991, IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz.

NCRP Report 86, Biological Effects and Exposure Criteria for Radiofrequency Electromagnetic Fields, National Council on Radiation Protection and Measurements, 1986.

HUMAN EXPOSURE TO RADIOFREQUENCY RADIATION: A COMPREHENSIVE REVIEW PERTINENT TO AIR FORCE OPERATIONS
http://www.brooks.af.mil/AFRL/HED/hedr/reports/human_exposure/htmlfile13.html